# Packet De-Duplication

Gigamon customers use network TAPs to gain 100 percent visibility into network traffic and traffic aggregation to achieve effective application, network, and security monitoring and analysis. This results in the elimination of blind spots and improves understanding of application performance, network utilization, and security threats. However by its nature, a traffic aggregation solution collects packets from multiple points within a network and along network paths, resulting in duplicate copies being sent to your tools for analysis. Duplicates can also be caused by inter-VLAN communication, incorrect switch configuration, or unavoidable SPAN/mirror port configurations. SPAN ports are really just another form of aggregation within a network switch.

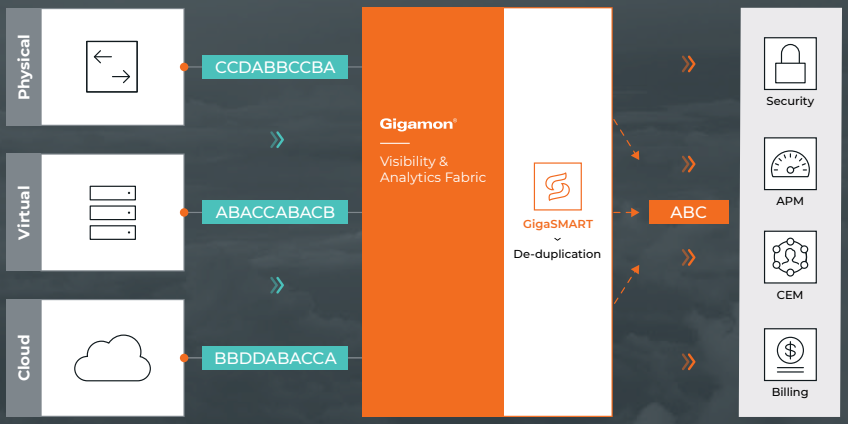


Figure 1. Tool optimization for physical, virtual, and cloud visibility with Packet De-duplication.

## KEY BENEFITS

- Eliminate redundant information currently feeding your network and security tools
- Gain improved value and performance from existing tools by deferring future upgrades
- Free tool storage and processing resources used to handle redundant packets in the traffic stream
- Improve tool performance, capacity, efficiency, and reliability
- Increase the time tools spend on packet analysis while reducing time spent de-duping packets
- Gain more accurate performance analysis
- Reduce false positive results for error reporting metrics, including packet retransmissions
- Reduce load due to elimination of duplicate packet storage
- Boost speed and accuracy of forensics analysis and malware detection

Since today's networks are already transporting traffic volumes at much higher rates than most tools can handle, analysis tools cannot easily handle the processing drain of 40 percent or more of duplicate packets on incoming feeds. This drain on network traffic processing is a real challenge needing an effective solution.

The impact of duplicate packets can create many challenges, including:

- Distorted results when evaluating application or network performance, leading to improper performance diagnosis and artificially elevated packet and byte counts
- Duplicate packets can be misinterpreted by analysis tools, resulting in false positives for problems that don't exist
- Reduced retention periods of data on forensic recorders due to the storage wastefully allocated to de-duplicate traffic
- Inaccurate and more voluminous flow data in NetFlow/IPFIX reports

## Gigamon Solution — Duplicate Packet Removal with GigaSMART

The GigaSMART® Packet De-duplication application identifies and eliminates duplicate packets and sends an optimized feed to the tools. It offloads the de-duplication task from the tools, allowing you to centralize the deduplication function and feed multiple tools with the same feed. Packet De-duplication significantly improves the performance of connected tools, allowing them to analyze increased volumes of aggregated traffic on the network without increasing tool capital expenditure.

GigaSMART Packet De-duplication is robust, accurate, and customizable. It allows you to tune duplicate detection to improve accuracy and effectiveness. For example, you can specify whether two packets that are identical except for IPTOS or TCP Sequence number are considered duplicates. In addition, the detection window is configurable between 10–50,000 µs.

Expected packet changes due to forwarding, including source and destination MAC addresses, are taken into consideration. The application also supports service chaining so that you can send the de-duplicated traffic stream to other GigaSMART applications, such as NetFlow for optimized NetFlow generation and export.

Packet De-duplication is supported as a GigaSMART application by GigaVUE® Cloud Suite™ for processing in public cloud or private cloud environments, and by GigaVUE HC Series for processing physically on premises.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com